University Paris-Saclay - IQUPS

Optical Quantum Engineering: From fundamentals to applications

Philippe Grangier,
Institut d'Optique, CNRS, Ecole Polytechnique.

- Lecture 1 (7 March, 9:15-10:45) :
  Qubits, entanglement and Bell's inequalities.
- Lecture 2 (14 March,11:00-12:30) :
  From QND measurements to quantum gates and quantum information.
- Lecture 3 (21 March, 9:15-10:45) :
  Quantum cryptography with discrete and continuous variables.
- Lecture 4 (28 March, 11:10-12:30) :
  Non-Gaussian quantum optics and optical quantum networks.

1. Bell's Inequalities : solution

1. By inverting the equations when $\phi = 0$ we get :

$$|+_z\rangle = \cos(\theta/2)|+_{\vec{u}}\rangle - \sin(\theta/2)|-_{\vec{u}}\rangle$$
$$|-_z\rangle = \sin(\theta/2)|+_{\vec{u}}\rangle + \cos(\theta/2)|-_{\vec{u}}\rangle$$

and thus (omitting the vector symbol) :

$$\begin{aligned} |+_z, -_z\rangle &= \cos(\theta_1/2)\sin(\theta_2/2)|+_a, +_b\rangle + \cos(\theta_1/2)\cos(\theta_2/2)|+_a, -_b\rangle \\ &- \sin(\theta_1/2)\sin(\theta_2/2)|-_a, +_b\rangle - \sin(\theta_1/2)\cos(\theta_2/2)|-_a, -_b\rangle \end{aligned}$$

$$\begin{aligned} |-_z, +_z\rangle &= \sin(\theta_1/2)\cos(\theta_2/2)|+_a, +_b\rangle - \sin(\theta_1/2)\sin(\theta_2/2)|+_a, -_b\rangle \\ &+ \cos(\theta_1/2)\cos(\theta_2/2)|-_a, +_b\rangle - \cos(\theta_1/2)\sin(\theta_2/2)|-_a, -_b\rangle \end{aligned}$$

and thus:

$$\begin{aligned} |\psi\rangle &= (\sin((\theta_2 - \theta_1)/2)|+_a, +_b\rangle + \cos((\theta_2 - \theta_1)/2)|+_a, -_b\rangle \\ &- \cos((\theta_2 - \theta_1)/2)|-_a, +_b\rangle + \sin((\theta_2 - \theta_1)/2)|-_a, -_b\rangle)/\sqrt{2} \end{aligned}$$

2. a. Each measurement can give the results ± 1, so there are 4 possibilities $(+_a, +_b)$, $(+_a, -_b)$, $(-_a, +_b)$, et $(-_a, -_b)$ with probabilities :

$$P_{++} = P_{--} = \frac{1}{2}\sin^2(\frac{\theta_2 - \theta_1}{2}), \quad P_{+-} = P_{-+} = \frac{1}{2}\cos^2(\frac{\theta_2 - \theta_1}{2})$$

2.b For one particle one sums the results for the other one, and thus

$$P_+ = P_{++} + P_{+-} = 1/2 \quad \text{et} \quad P_- = P_{-+} + P_{--} = 1/2$$

2.c $P_{cond} = P_{+-}/P_- = \cos^2((\theta_2 - \theta_1)/2)$

2.d If $\theta_2 = \theta_1$ then $P_{cond} = 1$: full correlation between results.

2.e. $E_Q = P_{++} - P_{+-} - P_{-+} + P_{--}$: correlation function.

$$E_Q = -\cos^2((\theta_2 - \theta_1)/2) + \sin^2((\theta_2 - \theta_1)/2) = -\cos(\theta_2 - \theta_1) = -\vec{a}.\vec{b}$$

Si $|E_Q| = 1$ again full correlation (or anticorrelation) between the results.

3. $A(\lambda, \vec{a})$ et $A(\lambda, \vec{a}')$ are either equal or opposite in sign.
- if equal $A(\lambda, \vec{a}) + A(\lambda, \vec{a}') = \pm 2$ and $A(\lambda, \vec{a}) - A(\lambda, \vec{a}') = 0$, so $s(\lambda) = \pm 2$
- if opposite$A(\lambda, \vec{a}) + A(\lambda, \vec{a}') = 0$ and $A(\lambda, \vec{a}) - A(\lambda, \vec{a}') = \pm 2$, so $s(\lambda) = \pm 2$. The average of a quantity equal to ± 2 over a positive and normalized distribution must be between $+2$ and -2, hence the result.

4. For the indicated angles one has

$$S_Q = -3\cos(\theta) + \cos(3\theta) \quad \text{thus} \quad dS_Q/d\theta = 3(sin(\theta) - sin(3\theta)).$$

The derivative cancels for $3\theta = \theta + 2n\pi$, i.e. $\theta = n\pi$ (minimum), or $3\theta = \pi - \theta + 2n\pi$, i.e. $\theta = \pi/4 + n\pi/2$ (maximum).

One has thus $\theta = \pi/4$ ou $3\pi/4$, and

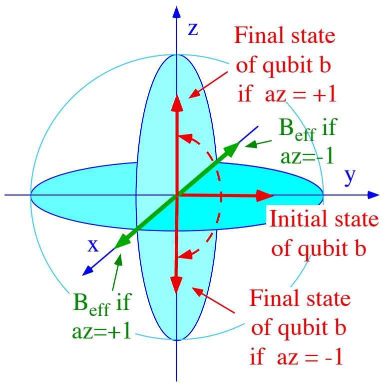
$$S_Q = -3\cos(\pi/4) + \cos(9\pi/4) = -4\cos(\pi/4) = -2\sqrt{2}.$$

Finally one has $|S_{Q,max}| = 2\sqrt{2} > 2$: conflict

2. QND measurement of a spin component : solution.

One wants to perform a QND measurement of $\hat{\sigma}_z$ on a qubit "a" : if the qubit is a spin 1/2 particle, one gets the spin "a" to interact with another spin "b" during a time τ, and read out the result on spin "b".

An appropriate interaction Hamiltonian is : $H_m = \hbar g\ \hat{\sigma}_{az}\ \hat{\sigma}_{bx}/2$



Everything happens as if qubit a creates on qubit b an effective magnetic field, aligned along Ox, with a sign depending on the state $|\pm\rangle_{az}$ (see exercise !).

$$|+\rangle_{az}\otimes|+\rangle_{by} \longrightarrow |+\rangle_{az}\otimes|+\rangle_{bz}$$
$$|-\rangle_{az}\otimes|+\rangle_{by} \longrightarrow i|-\rangle_{az}\otimes|-\rangle_{bz}$$

QND measurement of a spin component.

One wants to perform a measurement on a qubit "a" by using an indirect (rather than direct) measurement, called a "Quantum Non Demolition" (QND) measurement. For instance, if the qubit is a spin 1/2 particle, one will not use a Stern-Gerlach magnet, but rather get the spin "a" to interact with another spin "b" during a time τ, and read out the result on spin "b". After the interaction, one measures (directly) the state of qubit b, and one wants to infer the states of qubit a.
The spin observables of the two qubits are $\vec{\sigma}_{a,b}$ and

$$\sigma_{ax}|ax:\pm1\rangle = \pm|ax:\pm1\rangle,$$
$$\sigma_{ay}|ay:\pm1\rangle = \pm|ay:\pm1\rangle,$$
$$\sigma_{az}|az:\pm1\rangle = \pm|az:\pm1\rangle,$$

with the same definitions for b, and :

$$|ax:\pm\rangle = (|az:+\rangle\pm|az:-\rangle)/\sqrt{2},\quad |ay:\pm\rangle = (|az:+\rangle\pm i|az:-\rangle)/\sqrt{2}$$
$$|ay:\pm\rangle = ((1\pm i)|ax:+\rangle + (1\mp i)|ax:-\rangle)/2$$

2. The interaction is described by the hamiltonian $H_m = \hbar g\ \sigma_{az}\ \sigma_{bx}/2$, acting during a duration τ. The operators H_m, σ_{az} and σ_{bx} commute, and the eigenstates of H_m are $|az:\pm\rangle$ and $|bx:\pm\rangle$. The eigenvalues $\pm\hbar g/2$ are obtained by multiplying the eigenvalues of σ_{az} and σ_{bx}, which are a complete set of commuting observables.
3. The initial state of the pair of qubits is $|\psi_+(0)\rangle = |az:+\rangle\otimes|by:+\rangle$, and the duration of the interaction is $g\tau = \pi/2$. Calculate the system's final state $|\psi(\tau)\rangle$. Same question if the initial state is $|\psi_-(0)\rangle = |az:-\rangle\otimes|by:+\rangle$. Give an interpretation of these results by considering the expression of H_m and Bloch's sphere for the qubit b, in the two cases where the qubit a is in either of the two states $\{|az:\pm1\rangle\}$.

$$|\psi(0)\rangle = |az:+\rangle\otimes|by:+\rangle$$

$$\begin{aligned}|\psi_+(\tau)\rangle &= |az:+\rangle((1+i)e^{-ig\tau/2}|bx:+\rangle + (1-i)e^{ig\tau/2}|bx:-\rangle)/2\\ &= |az:+\rangle(|bx:+\rangle+|bx:-\rangle)/\sqrt{2} \qquad (\text{since } g\tau/2=\pi/4)\\ &= |az:+\rangle\otimes|bz:+\rangle\end{aligned}$$

In the same way $|\psi_-(\tau)\rangle = i|az:-\rangle\otimes|bz:-\rangle$. The state of qubit a does not change, and qubit b "copies" this state.

4. Starting from the initial state $|\psi(0)\rangle = (\alpha|az:+\rangle+\beta|az:-\rangle)\otimes|by:+\rangle$, one measures the spin component of qubit b along Oz, after the interaction has been carried out and turned off.
What are the possible results, and what are their probabilities ? After this measurement, what can be said about the component along Oz for qubit a ? Justify the name "QND measurement" given to this kind of process.

$|\psi(0)\rangle = (\alpha|az:+\rangle + \beta|az:-\rangle)\otimes|by:+\rangle$ and from the superposition principle :

$$|\psi(\tau)\rangle = (\alpha\ |az:+\rangle|bz:+\rangle + i\beta\ |az:-\rangle|bz:-\rangle)$$

This is a correlated state very close to the EPR state : a measurement on qubit gives $+1$ with probability $|\alpha|^2$ and -1 with probability $|\beta|^2$. For each result, the state of qubit a is perfectly known after the measurement ("reduction of the wave packet"). The quantum measurement of σ_{az} is done by an "indirect measurement", called a QND measurement.

3. Schmidt decomposition : solution.

1. One has :

$$|\psi_{AB}\rangle = \sum_{i,j} c_{ij}|u_i\rangle_A|v_j\rangle_B = \sum_i |u_i\rangle_A(\sum_j c_{ij}|v_j\rangle_B) = \sum_i |u_i\rangle_A|w_i\rangle_B$$

where we define $|w_i\rangle_B = \sum_j c_{ij}|v_j\rangle_B$.

2. One has $|\psi_{AB}\rangle\langle\psi_{AB}| = \sum_{i,j}(|u_i\rangle\langle u_j|)_A(|w_i\rangle\langle w_j|)_B$ and thus :

$$\begin{aligned}\rho_A &= \sum_{i,j,k}(|u_i\rangle\langle u_j|)_A\langle v_k|w_i\rangle\langle w_j|v_k\rangle \\ &= \sum_{i,j,k}(|u_i\rangle\langle u_j|)_A\langle w_j|v_k\rangle\langle v_k|w_i\rangle \\ &= \sum_{i,j}(|u_i\rangle\langle u_j|)_A\langle w_j|w_i\rangle\end{aligned}$$

where we used the closure relation $\sum_k |v_k\rangle\langle v_k| = I$.

3. It is assumed that $\rho_A = \sum_i p_i \,(|u_i\rangle|\langle u_i|)_A$, and this by using the result of the previous question :
$\langle w_j|w_i\rangle = 0$ if $i \neq j$, therefore the vectors $\{|w_i\rangle\}$ are orthogonal.
$\langle w_i|w_i\rangle = p_i$, so the norm of $|w_i\rangle$ is equal to $\sqrt{p_i}$.

4. Defining $|\tilde{w}_j\rangle = |w_j\rangle/\sqrt{p_j}$ the vectors $\{|\tilde{w}_j\rangle_B\}$ are normalized and orthogonal, and one has :

$$|\psi_{AB}\rangle = \sum_i \sqrt{p_i}\, |u_i\rangle_A|\tilde{w}_i\rangle_B$$

5. Using the Schmidt decomposition of the state $|\psi_{AB}\rangle$ one gets :

$$\rho_B = \sum_i p_i \,(|\tilde{w}_i\rangle\langle\tilde{w}_i|)_B.$$

The reduced density matrix ρ_A et ρ_B have the same non-zero eigenvalues, which are p_i.

6. The Schmidt number is equal to one iff $|\psi_{AB}\rangle = |\phi_A\rangle|\chi_B\rangle$, which is true iff $|\psi_{AB}\rangle$ is separable.

4. Security of quantum cryptography: solution

1. Mutual informations I_{BA} and I_{BE} :

$I_{BA} = H(B_X) - H(B_X|A)$ et $I_{BE} = H(B_X) - H(B_X|E)$.

and therefore $\Delta I = I_{AB} - I_{BE} = H(B_X|E) - H(B_X|A)$.

2. Starting from a pure entangled state, Bob will receive a pure state conditioned by Alice's and Eve's measurement. One can then use the entropic inequalities and thus $H(B_X|A,E) + H(B_Y|A,E) \geq -2\log_2 c$.

Since the entropies can only increase when igoring (deleting) part of the information one has

$$H(B_X|E) + H(B_Y|A) \geq -2\log_2 c$$

3. Using $H(B_X|E) \geq -2\log_2 c - H(B_Y|A)$ one gets :

$$\Delta I \geq -2\log_2 c - H(B_X|A) - H(B_Y|A) = -2\,(\log_2 c + H(B|A)).$$

The protocol will be secure if $\Delta I > 0$, this is obtained when $\log_2 c + H(B|A) < 0$ or also $H(B|A) < -\log_2 c$

4. For the BB84 protocol one has $c = 1/\sqrt{2}$ and thus $-\log_2 c = 1/2$.
The protocol will be secure if $H(B|A) < 1/2$.
Since $H(B) = 1$ (isotropic density matrix), one has :

$$I_{AB} = H(B) - H(B|A) > 1/2.$$

5. One has $I_{AB} = 1 - H(e)$, où $H(e) = -e\log_2 e - (1-e)\log_2(1-e)$.
Therefore one require $1 - H(e) > 1/2$, or also $H(e) < 1/2$ (could be directly obtained from $H(B|A) < 1/2$). By plotting $H(e)$ one sees that this condition corresponds to $e < 11\%$. Note that $I_{AB} = 1 - H(e)$ is the channel capacity of a binary channel with errors, and that $I_{AB} + I_{BE} \leq 1$.

IQUPS – Lecture 3 – P. Grangier

Lecture 3 - Quantum cryptography (discrete and continuous) (Tuesday 21/03)

2.1 Quantum cryptography : basic ideas.

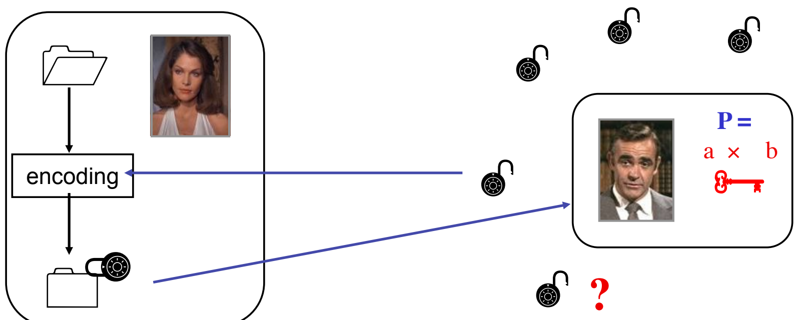
2.2 Continuous variable quantum cryptography : principles

2.3 Continuous variable quantum cryptography : implementations

The characters

Public key cryptosystems

Rivest, Shamir et Adelman (RSA, 1978)



What is inside the « public key » ?
the product P of two large numbers :
factorization very difficult to perform !

PUBLIC KEY CRYPTOSYSTEMS

- Public key cryptosystems (1970's) :
Security due to the difficulty to perform the calculation required to break the code. Usual exemple : "RSA" code (Rivest, Shamir and Adleman, 1978)

a and b two large prime numbers → easy calculation → p = a.b, q = (a-1).(b-1), r and s so that gcd(q, s) = 1 et r . s ≡ 1 modulo q

- Bob **sends openly p and r (the key)**, and keeps q and s
- For coding "x", Alice calculates $y = x^r$ modulo p and sends openly "y"
- Surprising result of numbers theory : $x = y^s$ modulo p ok for Bob !

But the eavesdropper (Eve) does not know s, q, a, b, and cannot do anything, *because the calculation of a and b from p requires an exponential time with the best present algorithms.* (unfeasible when p has more than 200 digits)

Factorising RSA 155 (512 bits - summer 1999)

« Challenge » proposed the RSA company (www.rsa.com)
Previous record : RSA140 (465 bits), february 1999

RSA155 = 109417386415705274218097073220403576120037329454492\
059909138421314763499842889347847179972578912673324976257528\
997818337970765372440271467435315933543338897;

RSA155 is not a prime ! ("probabilistic" algorithm, very fast)

Factorization ?	**Preparation :**	9 weeks over 10 workstations.
	Sieve :	3.5 months over 300 PCs , 6 countries
	Result :	**3.7 Go, stored in Amsterdam**
	Processing :	9.5 days on Cray C916, Amsterdam
	Factorization:	39.4 hours on 4 workstations

f1 = 102639592829741105772054196573991675\
900716567808038066803341933521790711307779;
f2 = 106603488380168454820927220360012878\
679207958575989291522270608237193062808643;

f1 and f2 are primes, and f1 * f2 = RSA155 (immediate on PC)

« Challenges » proposed by the company RSA

Number	bits	digits	date completed	sieving time	algorithm
C116		116	1990	275 MIPS years	mpqs
RSA-120	398	**120**	June, 1993	830 MIPS years	mpqs
RSA-129	428	**129**	April, 1994	5000 MIPS years	mpqs
RSA-130	431	**130**	April, 1996	1000 MIPS years	gnfs
RSA-140	465	**140**	February, 1999	2000 MIPS years	gnfs
RSA-512	**512**	155	August, 1999	8000 MIPS years	gnfs
C158		158	January, 2002	3.4 Pentium 1GHz CPU years	gnfs
RSA-160	530	**160**	March, 2003	2.7 Pentium 1GHz CPU years	gnfs
RSA-576	**576**	174	December, 2003	13.2 Pentium 1GHz CPU years	gnfs
C176		176	May, 2005	48.6 Pentium 1GHz CPU years	gnfs
RSA-200	663	**200**	May, 2005	121 Pentium 1GHz CPU years	gnfs
RSA-768	**768**	232	Dec, 2009	3,300 Opteron 1GHz CPU years	gnfs

Improvement by three orders of magnitude between 1999 and 2009...

PUBLIC KEY CRYPTOSYSTEMS

- Problems :

- Mathematical demonstrations about PKC have a statistical character (the factorisation may be found easily for "unfortunate choices" of a, b)

--> "recommendations" for the choice of the prime numbers a and b

- **No absolute demonstration for security** -> better computers, better algorithms (obviously kept secret) ?

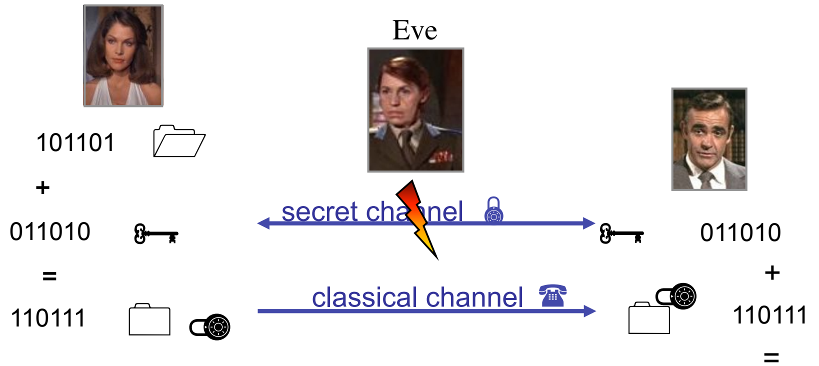
- Article by Peter Shor (1994) :

a "quantum computer" might be able to factorize the product of two prime numbers in a "polynomial" time ! *lot of reactions !*

Best classical algorithm (number field sieve) :
nfs[n] = Exp[1.9 Log[n]$^{1/3}$ Log[Log[n]]$^{2/3}$] **nfs[2^{1024}] / nfs[2^{512}] = 6.2 10^6**

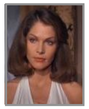
Shor algorithm : shor[n] = Log[n]^3 **shor[2^{1024}] / shor[2^{512}] = 8**

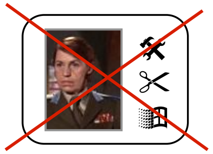
Secret key cryptosystem : one-time pad (G. Vernam, 1917)



Demonstrably secure if the key is :
- random
- as long as the message
- used only once (Shannon)

Quantum Secret Key Cryptosystem : Bennett-Brassard (1984)



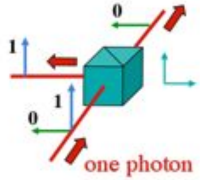


101101		
+	quantum channel	011010
011010		+
=	classical channel	110111
110111		=
		101101

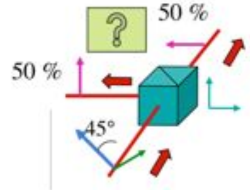
Demonstrably secure if the key is :
- random
- as long as the message
- used only once (Shannon)
- **unknown by Eve : Quantum laws !**

Polarization of a Single Photon

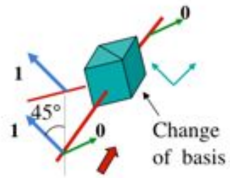
Coding a bit (0 or 1) on the polarization of one photon



Deterministic result



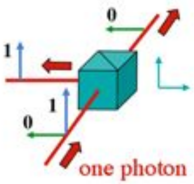
Random result



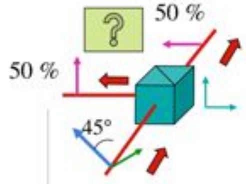
Deterministic result

Polarization of a Single Photon

Coding a bit (0 or 1) on the polarization of one photon

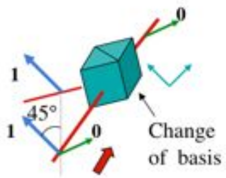


Deterministic result



Random result

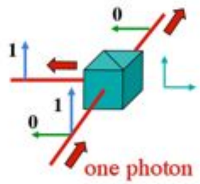
A useful information is extracted if and only if the basis used by the emitter (coding) and by the receiver (detecting) are the same !



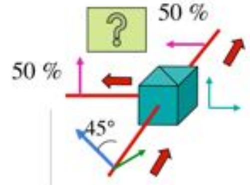
Deterministic result

Polarization of a Single Photon

Coding a bit (0 or 1) on the polarization of one photon



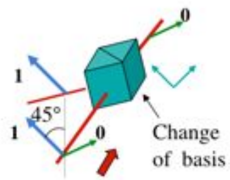
Deterministic result



Random result

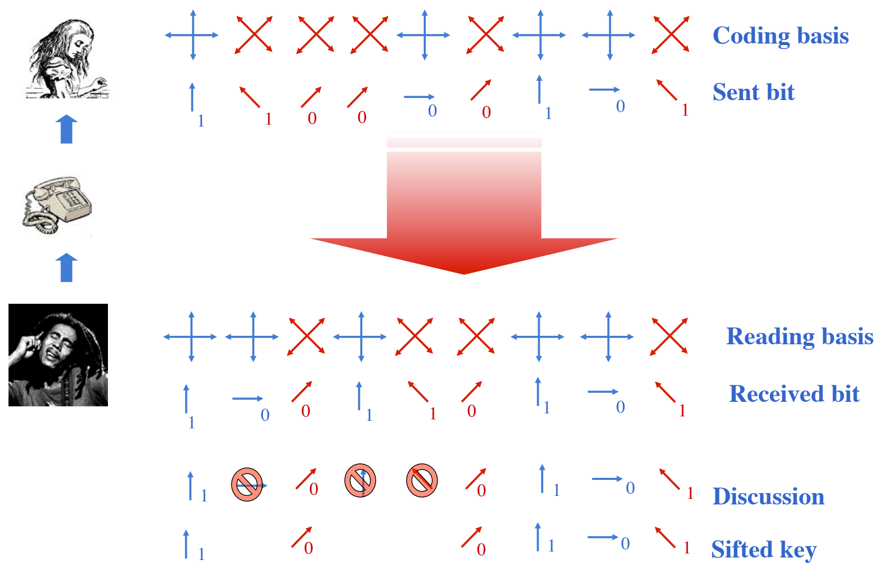
The polarization of a single photon carries a "quantum bit" or "qubit"

$$|45°\rangle = (|h\rangle + |v\rangle)/\sqrt{2}$$
$$|135°\rangle = (|h\rangle - |v\rangle)/\sqrt{2}$$

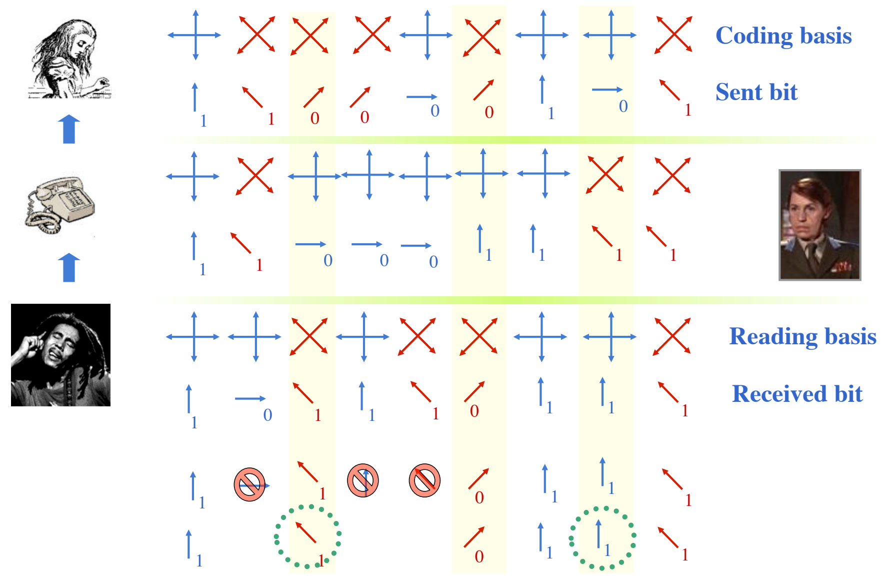


Deterministic result

« BB84 » Protocol (Bennett and Brassard, 1984)



« BB84 » Protocol (Bennett and Brassard, 1984)



QUANTUM CRYPTOGRAPHY : PRINCIPLE
(C. Bennett and G. Brassard, 1984)

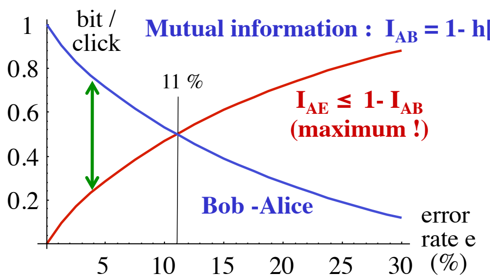
Eve has to make a measurement without knowing the basis used by Alice (this information comes too late for her !)

- intercept / resend using either the + or x basis
- intercept / resend using an optimized basis (22.5°)
- use quantum non-demolition measurements…
- duplicate (clone) photons and keep one aside…

All such measurements will create errors in the transmission (the more Eve knows, the more errors !)

Mutual information : I_{AB} = 1- h[e]

h[e] = - e $\log_2$[e] - (1-e) $\log_2$[1-e]
binary entropy



Size of the secret key : K = I_{AB} - I_{AE}

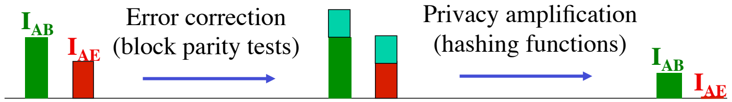
If Eve has all power allowed by quantum mechanics, she will get less information than Bob as long as the error rate is smaller than 11%

QUANTUM CRYPTOGRAPHY : PRINCIPLE
(C. Bennett and G. Brassard, 1984)

5 - Classical post-processing (essential for security !)
Requires a public authenticated channel

*** Evaluation of errors :**
After the initial exchange between Alice and Bob measure the error rate by comparing publicly a part of the raw key:
-> evaluation of the amount of information (maybe) available to Eve.

*** Error correction and privacy amplification (possible if I_{AB} > I_{AE} !)**
Then Alice and Bob extract the available key by correcting errors and eliminating Eve's residual knowledge (this reduces the size of the key)



6 - Alice and Bob have a totally secure and errorless secret key (non-zero size if initial QBER < 11%)

Industrial Perspectives ?

* **Several startups worldwide are selling QKD systems** (optical fibers, 50 km)

IdQuantique (Genève)

MagiQ Technologies (New York)

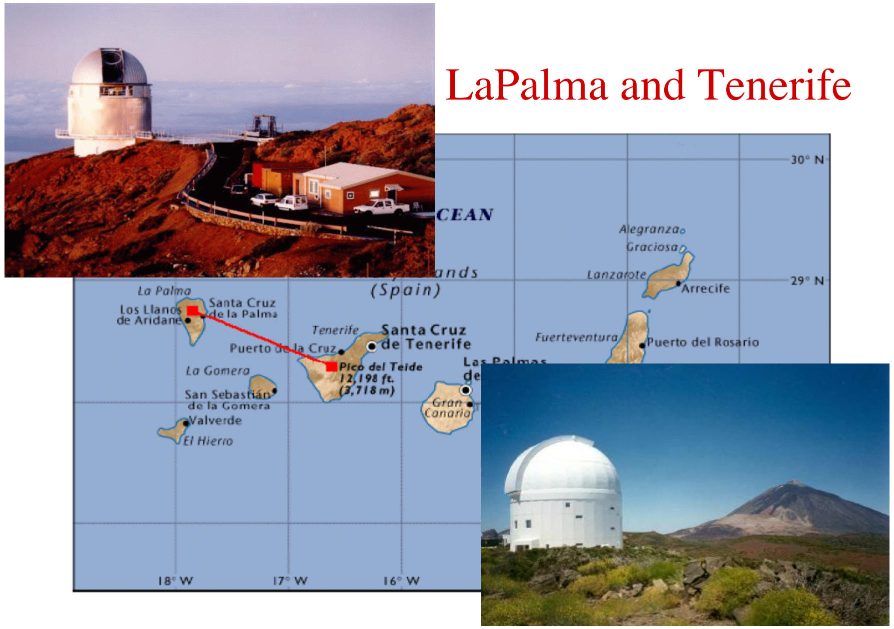
* **Intense activity in the USA (mostly military) and in Japan (NEC, Fujitsu…)**

* **In Europe « Integrated Project » SECOQC :**

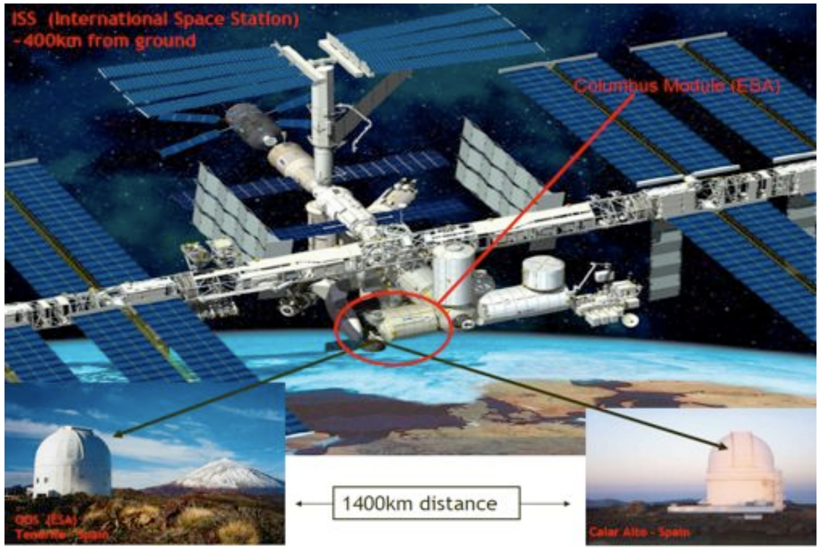
« Secure Communication based on Quantum Cryptography ».

Urban networks demonstrated in Vienna (2008) and Tokyo (2010, 2015...)

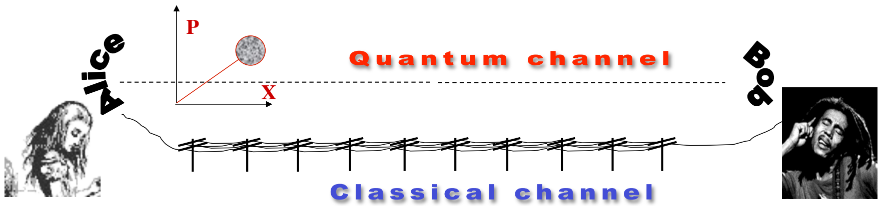
LaPalma and Tenerife



Quantum cryptography with satellites



Coherent States Quantum Key Distribution



* Essential feature : quantum channel with non-commuting quantum observables

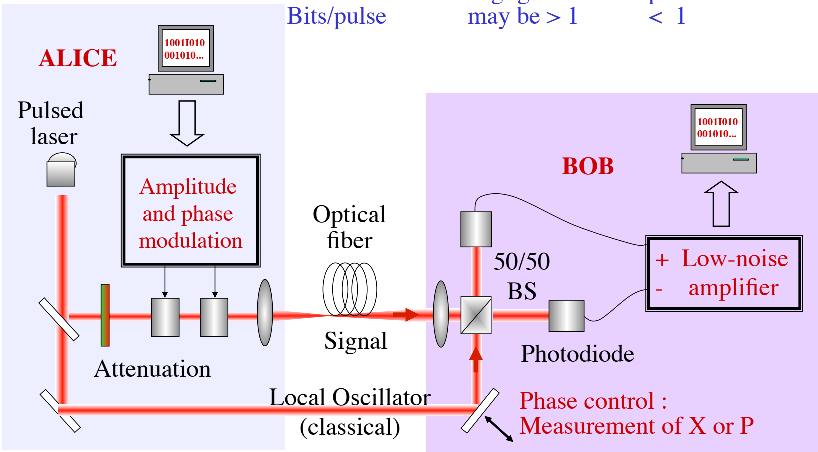
-> not restricted to single photon polarization or phase !

-> Design of Continuous-Variable QKD protocols where :

* The non-commuting observables are the quadrature operators X and P
* The transmitted light contains weak coherent pulses (about 10 photons) with a gaussian modulation of amplitude and phase
* The detection is made using shot-noise limited homodyne detection

Coherent States Quantum Key Distribution

	Homodyne	Counting (APD)
Efficiency	> 90%	10-50 %
Dark rate	negligible	problem
Bits/pulse	may be > 1	< 1



QKD protocol using coherent states with gaussian amplitude and phase modulation

Efficient transmission of information using continuous variables ?

-> Shannon's formula (1948) : the mutual information I_{AB} (unit : bit / symbol) for a gaussian channel with additive noise is given by

$$I_{AB} = 1/2 \ \log_2 [\, 1 + V(signal) / V(noise) \,]$$

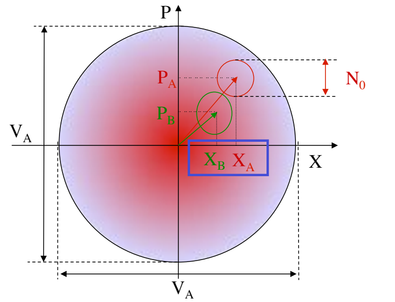
Reminder : I(X; Y) =
H(X) - H(X | Y) =
H(Y) - H(Y| X) =
H(X) + H(Y) - H(X; Y)

(a) Alice chooses X_A and P_A within two random gaussian distributions.

(b) Alice sends to Bob the coherent state $| X_A + i P_A >$

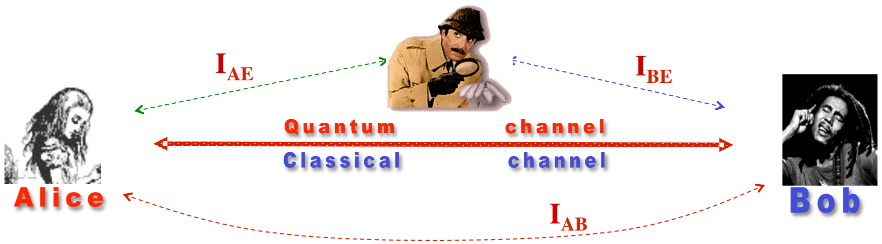
(c) Bob measures either X_B or P_B

(d) Bob and Alice agree on the basis choice (X or P), and keep the relevant values.



Data Reconciliation

how to correct errors, revealing as less as possible to Eve ?

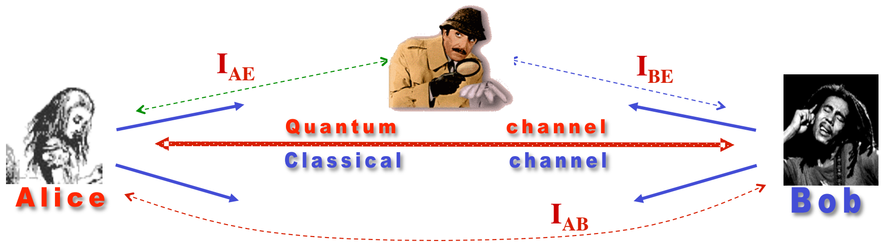


Main idea (Csiszar and Körner 1978, Maurer 1993) :

Alice and Bob can in principle distill, from their correlated key elements, a common secret key of size $S > \sup(I_{AB} - I_{AE}, I_{AB} - I_{BE})$ bits per key element.

Crucial remark : it is enough that I_{AB} is larger than the **smallest** of I_{AE} and I_{BE} (i.e. one has to take the best possible case).

Data Reconciliation



If I_{AE} is the smallest, the reconciliation must keep $S = I_{AB} - I_{AE}$ constant :
Alice gives correction data to Bob (and also to Eve),
and Bob corrects his data :
« direct reconciliation protocol »

If I_{BE} is the smallest, the reconciliation must keep $S = I_{AB} - I_{BE}$ constant :
Bob gives correction data to Alice (and also to Eve),
and Alice corrects his data :
« reverse reconciliation protocol »

Crucial question for Alice and Bob :
how to bound I_{AE} and I_{BE}, knowing I_{AB} ?

Direct reconciliation

Bounding I_{AE} (F. Grosshans and P. Grangier, *PRL* **88**, 057902 (2002)).

$$I_{AB} = 1/2 \ \log_2 [1 + V_A / (N_0 + N_{eqB})]$$

$$I_{AE} = 1/2 \ \log_2 [1 + V_A / (N_0 + N_{eqE})]$$

where
- V_A : variance of Alice's modulation
- N_0 : shot noise (coherent state)
- N_{eqB} : « equivalent channel noise » on Bob's side
- N_{eqE} : « equivalent channel noise » on Eve's side

see e.g. : P. Grangier et al., Nature **396**, 537 (1998).

From Heisenberg $N_{eqB} N_{eqE} \geq N_0^2$ (no cloning !) and thus :

$$I_{AE} \leq (I_{AE})_{best} = 1/2 \ \log_2 [1 + V_A / (N_0 + N_0^2 / N_{eqB})]$$

Key size : $S = I_{AB} - (I_{AE})_{best}$

Reverse Reconciliation

Bounding I_{BE} (F. Grosshans et al., *Nature* **421**, 238 (2003))

How well can Alice and Eve infer Bob's measurement results ?

Define the « conditional variance » $V(X_B | X_E) = V(X_B) - |\langle X_B X_E \rangle|^2 / V(X_E)$

Conditional variances are also bounded by Heisenberg relations :

$$V(X_B|X_A)_{min} \, V(P_B|P_E) \geq N_0^2 \qquad V(P_B|P_A)_{min} \, V(X_B|X_E) \geq N_0^2$$

Using again Shannon's theorem… (and some algebra…)

$$I_{BE} \leq (I_{BE})_{best} = 1/2 \ \log_2 [T^2 (N_{eqB} + N_0 + V_A) / (N_{eqB} + N_0^2 / (N_0 + V_A))]$$

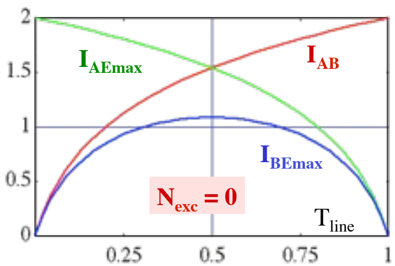
Key size : $S = I_{AB} - (I_{BE})_{best}$

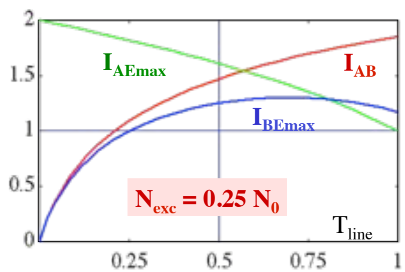
Summary on reconciliation protocols

The noise seen by Bob can be split in two parts (known by Alice and Bob !):

$$N_{eqB} = N_{losses} + N_{excess} = N_0 (1 - T_{line}) / T_{line} + N_{exc}$$

Mutual information (bits / symbol) for V_A=15 N_0



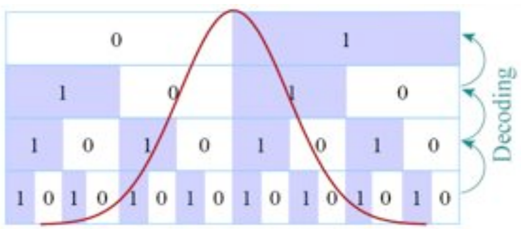


* I_{AE} : relevant for direct reconciliation, requires $T_{line} > 0.5$ and $N_{exc} < N_0$

* I_{BE} : relevant for reverse reconciliation, requires $N_{exc} < 0.5 \, N_0$

can be secure for any line transmission !

Reconciliation of correlated Gaussian variables

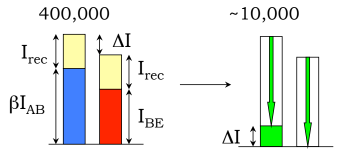


- Each level has a different error rate
- Non-independent levels

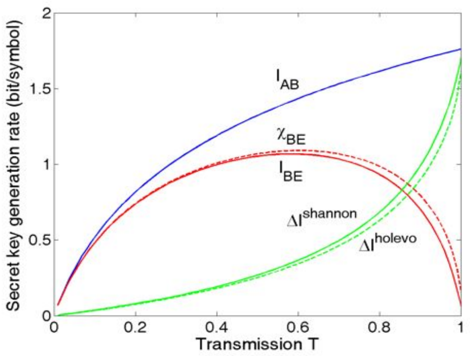
→ Error correction performed using multi-level iterative soft decoding with LDPC codes

G. Van Assche et al, IEEE Trans. on Inf. Theory 50, 394 (2004)
M. Bloch et al, arXiv:cs.IT/0509041 (2005)

- Standard privacy amplification based on universal hash functions
- Small processing time



Security of coherent state CV-QKD : collective attacks



Alice-Bob mutual information : I_{AB}

Eve-Bob mutual information :

I_{BE} (Shannon : individual attacks)

χ_{BE} (Holevo : collective attacks)

Secret Key Rate :

$\Delta I = I_{AB} - I_{BE}$ (Shannon)

$\Delta I = I_{AB} - \chi_{BE}$ (Holevo)

- For both individual and collective attacks Gaussian attacks are optimal → Alice and Bob consider Eve's attacks Gaussian and estimate her information using the Shannon quantity I_{BE} or the Holevo quantity χ_{BE}

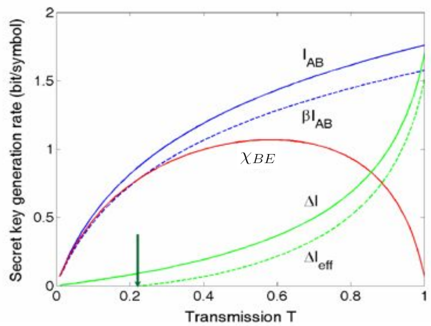
Fig : V_A = 21 (shot noise units)
ε = 0.005 (shot noise units), η = 0.5

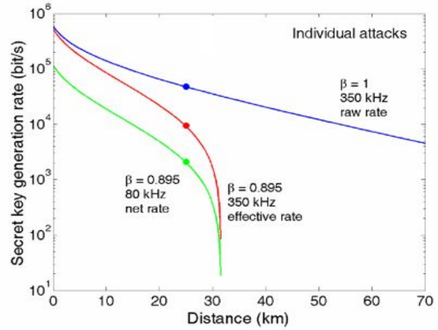
M. Navasqués et al, Phys. Rev. Lett. 97, 190502 (2006)
R. García-Patrón et al, Phys. Rev. Lett. 97, 190503 (2006)

Error correcting codes efficiency

Error correction with LDPC codes, efficiency β

$$\Delta I^{eff} = \beta I_{AB} - \chi_{BE}$$





Imperfect correction efficiency induces a limit to the secure distance

Security Proofs of CVQKD : summary

Secret bit rate K (bits/pulse) for information-theoretic security (Devetak, Winter, Renner...) :

$$K = \beta I_{AB} - \chi_{BE}$$

I_{AB} = Shannon's mutual information obtained by Alice and Bob after the quantum exchange. For a Gaussian modulation with variance V(signal)

I_{AB} = ½ Log_2[1 +V(signal)/V(noise)] = ½ Log_2[1 + SNR]

β = « Reconciliation efficiency » : fraction of I_{AB} that Alice and Bob can really extract after binarization of the data and error correction (difficult for low SNR !).

Using very good / state-of-the-art error correcting codes (LDPC) one gets β up to 95 %

χ_{BE} = Holevo information between Eve and Bob (« reverse reconciliation »)

Basic tool : Gaussian optimality (Cerf, Cirac...) : for a given transmission and noise of the channel, the best possible attack by Eve is a Gaussian attack : then the Holevo quantity can be calculated easily from the channel covariance matrix.

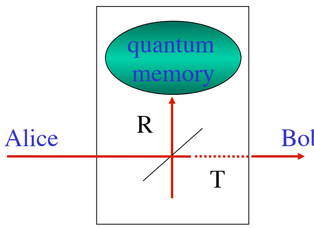
NB : This proof and formula are valid in the "asymptotic limit" of Alice and Bob exchanging an infinite amount of data. For a (more realistic) finite amount of data, the security proofs must use other techniques (smooth min entropy, introduced by Renato Renner).
See e.g. A. Leverrier et al, Phys. Rev. Lett. 110, 030502 (2013) & 114, 070501 (2015)

Institut d'Optique

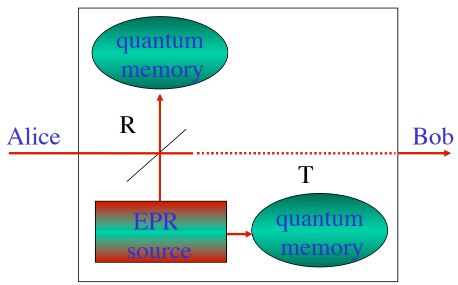
Eve's attacks

QIPC

Attacks considered in our proof are **individual gaussian attacks** (not easy !)



Eve's best attack against
direct reconciliation :
cloning machine (= BS)
+ quantum memory
N_{eqB} = (T/R) N_0
N_{eqE} = (R/T) N_0



Eve's best attack against
reverse reconciliation :
« entangling cloner »
+ quantum memories

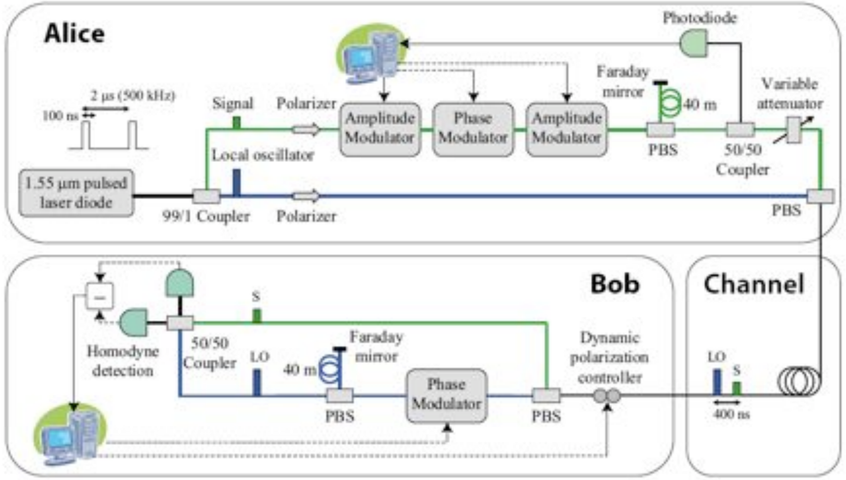
Security of coherent state CV-QKD protocol

- Security initially proven against (arbitrary) individual attacks :
  F. Grosshans et al, Nature 421, 238 (2003)
  F. Grosshans and N. J. Cerf, Phys. Rev. Lett. 92, 047905 (2004)
- Then security proven against arbitrary collective attacks :
  F. Grosshans, Phys. Rev. Lett. 94, 020504 (2005)
  M. Navasqués and A. Acin, Phys. Rev. Lett. 94, 020505 (2005)
- For both individual and collective attacks Gaussian attacks are optimal
  → Alice and Bob consider Eve's attacks Gaussian and estimate her information using the Shannon quantity I_{BE} or the Holevo quantity χ_{BE}
  M. Navasqués et al, Phys. Rev. Lett. 97, 190502 (2006)
  R. Garcia-Patrón et al, Phys. Rev. Lett. 97, 190503 (2006)

- **Finite size effects (needed for real experiments !) :**
  A. Leverrier, F. Grosshans and P. Grangier, Phys. Rev. A 81, 062343 (2010)
  P. Jouguet, S. Kunz-Jacques, E. Diamanti, A. Leverrier, Phys. Rev. A 86, 032309 (2012)
- **Coherent attacks and composable security proofs :**
  R. Renner and J.I. Cirac, Phys. Rev. Lett. 102, 110504 (2009)
  F. Furrer et al, Phys. Rev. Lett. 109, 100502 (2012)
  A. Leverrier et al, Phys. Rev. Lett. 110, 030502 (2013)
  Anthony Leverrier, Phys. Rev. Lett. 114, 070501 (2015)

All-fibered CVQKD @ 1550 nm

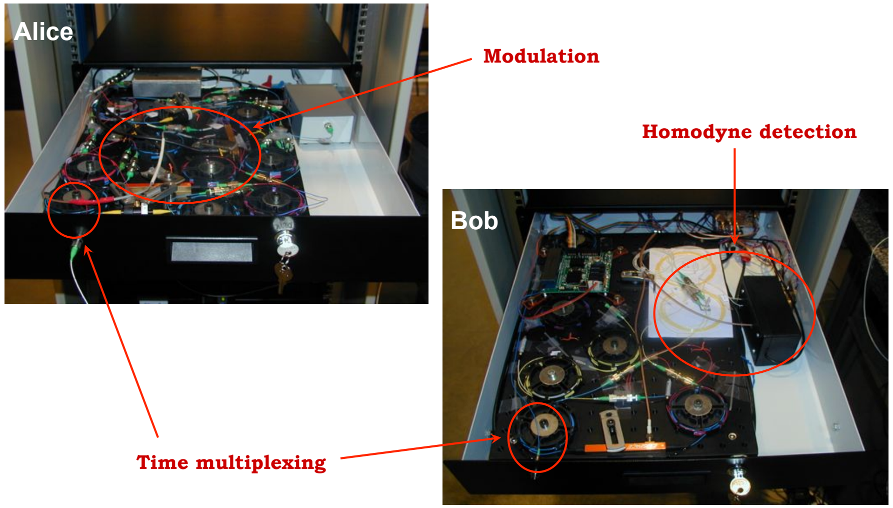
SECOQC



Field test of a continuous-variable quantum key distribution prototype
S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri and P Grangier
New J. Phys. 11 No 4, 04502 (April 2009)

All-fibered CVQKD @ 1550 nm

SECOQC

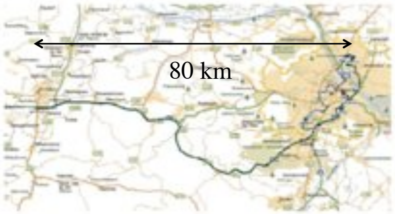


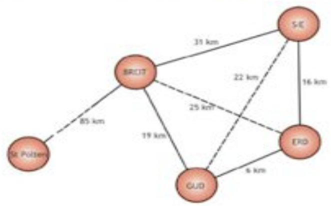
Quantum Back-Bone demonstrator SECOQC, Vienna, 8 october 2008

SECOQC

Development of a Global Network for Secure Communication based on Quantum Cryptography
www.secoqc.net

Real-size demonstration of a **secure quantum cryptography network**
by the European Integrated Project SECOQC, Vienna, 8 october 2008





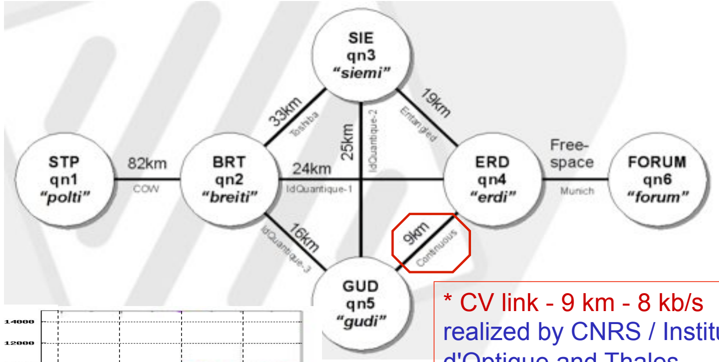
Node server

Continuous Variables

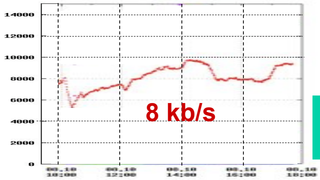
Id Quantique

The SECOQC Quantum Back Bone

Real-size demonstration of a **secure quantum cryptography network** by the European Integrated Project SECOQC, Vienna, 8 october 2008



* CV link - 9 km - 8 kb/s realized by CNRS / Institut d'Optique and Thales

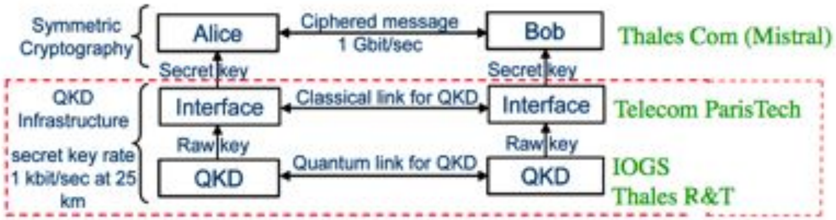


CV secret bit rate during the demo (8h)

SEQURE

Secure Encryption with QUantum key REnewal

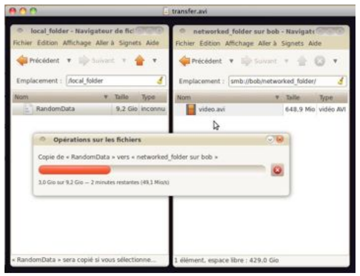
- Combining QKD (1 kbit/sec) with fast symmetric encryption (1 Gbit/sec)
- Use 128 bits AES, change key every 10 seconds



THALES · TELECOM ParisTech · INSTITUT d'OPTIQUE GRADUATE SCHOOL · SEQURENET A Quantum Key to Network Security

Symmetric Encryption with QUantum key REnewal

- Thales : Mistral Gbit
  (fast dedicated AES encryptor)



User window : « sequre drag and drop »

Complete set-up

SEQURE · THALES · TELECOM ParisTech · INSTITUT d'OPTIQUE GRADUATE SCHOOL · SEQURENET A Quantum Key to Network Security

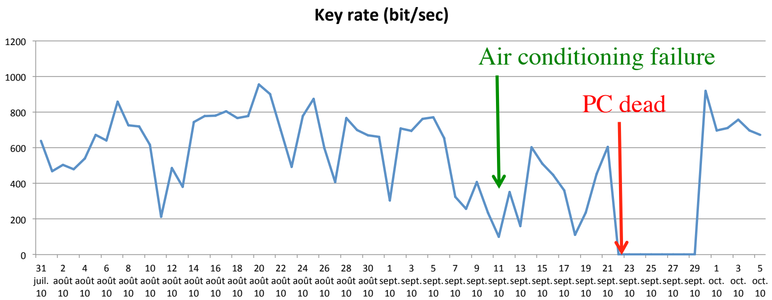
Field implementation

- Fibre link : Thales R&T (Palaiseau) <-> Thales Raytheon Systems (Massy)
- Fiber length about 12 km, 5.6 dB loss

SEQURE · THALES · TELECOM ParisTech · INSTITUT d'OPTIQUE GRADUATE SCHOOL · SEQURENET A Quantum Key to Network Security

Results

On site, 12 km distance, 5.6 dB loss
Minimal direct action on hardware (feedback loops, remote control)



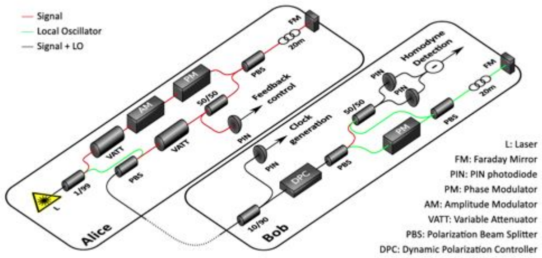
See http://www.demo-sequre.com

SEQURE THALES TELECOM ParisTech INSTITUT d'OPTIQUE GRADUATE SCHOOL SEQURENET A Quantum Key to Network Security

Implementation of coherent states CV-QKD

Fibered device : 1550 nm, only telecom components (no photon counters !),
Range 80 km: P. Jouguet et al, Nature Photonics 7, 378 (2013)

Optimized error correction, Graphic Processing Units (GPU) rather than CPU
=> Lot of calculations, but they do not limit the secret bit rate !
=> Up to 95% of Shannon's limit for any SNR : **longer distance**



SEQURENET A Quantum Key to Network Security

CYGNUS (commercial product)

Quantum Hacking

NTNU Department of Electronics and Telecommunications — UNIK University Graduate Center

- Several recent exemples of "quantum hacking" (e.g. Vadim Makarov et al.)
- Exploits weaknesses in single photon detectors
- Will NOT work against CVQKD (PIN photodiodes, linear regime)
- Hackers will have to work harder...
- ... and Trojan attacks will not make it (work under way, SQN + U. Erlangen)

Many other works on CVQKD !
<= Theory and Experiments :
(incomplete list !)

arXiv.org > quant-ph > arXiv:1106.0825
Quantum Physics
Security of Post-selection based Continuous Variable Quantum Key Distribution against Arbitrary Attacks
Nathan Walk, Thomas Symul, Timothy C. Ralph, Ping Koy Lam
(Submitted on 4 Jun 2011)

arXiv.org > quant-ph > arXiv:1011.0304
Quantum Physics
Continuous variable quantum key distribution in non-Markovian channels
Ruggero Vasile, Stefano Olivares, Matteo G A Paris, Sabrina Maniscalco
(Submitted on 1 Nov 2010)

arXiv.org > quant-ph > arXiv:0904.1694
Quantum Physics
Feasibility of continuous-variable quantum key distribution with noisy coherent states
Vladyslav C. Usenko, Radim Filip
(Submitted on 10 Apr 2009 (v1), last revised 21 Jan 2010 (this version, v2))

arXiv.org > quant-ph > arXiv:0904.1327
Quantum Physics
Security bound of continuous-variable quantum key distribution with noisy coherent states and channel
Yong Shen, Jian Yang, Hong Guo
(Submitted on 8 Apr 2009 (v1), last revised 29 Jun 2009 (this version, v2))

arXiv.org > quant-ph > arXiv:0903.0750
Quantum Physics
Confidential direct communications: a quantum approach using continuous variables
Stefano Pirandola, Samuel L. Braunstein, Seth Lloyd, Stefano Mancini
(Submitted on 4 Mar 2009)

arXiv.org > quant-ph > arXiv:1006.1257
Quantum Physics
A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution
Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, A. I. Lvovsky, Liang Tian
(Submitted on 7 Jun 2010 (v1), last revised 16 Jul 2010 (this version, v2))

arXiv.org > quant-ph > arXiv:0910.1042
Quantum Physics
A 24 km fiber-based discretely signaled continuous variable quantum key distribution system
Quyen Dinh Xuan, Zheshen Zhang, Paul L. Voss
(Submitted on 6 Oct 2009)

arXiv.org > quant-ph > arXiv:0811.4756
Quantum Physics
Feasibility of free space quantum key distribution with coherent polarization states
D. Elser, T. Bartley, B. Heim, Ch. Wittmann, D. Sych, G. Leuchs
(Submitted on 28 Nov 2008 (v1), last revised 13 Mar 2009 (this version, v2))

arXiv.org > quant-ph > arXiv:0705.2627
Quantum Physics
Experimental Demonstration of Post-Selection based Continuous Variable Quantum Key Distribution in the Presence of Gaussian Noise
Thomas Symul, Daniel J. Alton, Syed M. Assad, Andrew M. Lance, Christian Weedbrook, Timothy C. Ralph, Ping Koy Lam
(Submitted on 18 May 2007)